FortiManager - Release Notes

Version 6.4.3

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

November 16, 2021
FortiManager 6.4.3 Release Notes
02-643-667558-20211116

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-10-22	Initial release.
2020-11-02	Updated Known Issues on page 37.
2020-11-16	Added support for FortiADC and FortiSOAR.
2020-11-18	Updated FortiManager VM firmware on page 11.
2020-11-26	Updated Resolved Issues on page 29 and Known Issues on page 37.
2021-02-18	Updated Supported models on page 6.
2021-02-22	Updated Virtualization on page 17.
2021-03-04	Added Management extension applications on page 7.
2021-04-12	Added FortiManager VM subscription license on page 6.
2021-05-07	Upgraded Downgrading to previous firmware versions on page 11.
2021-11-16	Updated Resolved Issues on page 29.

FortiManager 6.4.3 Release

This document provides information about FortiManager version 6.4.3 build 2201.

The recommended minimum screen resolution for the FortiManager GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

This section includes the following topics:

Supported models

FortiManager version 6.4.3 supports the following models:

FortiManager	FMG-200F, FMG-300E, FMG-300F, FMG-400E, FMG-1000F, FMG-2000E, FMG-3000F, FMG-3700F, FMG-3900E, and FMG-4000E.
FortiManager VM	FMG-VM64, FMG-VM64-Ali, FMG-VM64-AWS, FMG-VM64-AWSOnDemand, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

FortiManager VM subscription license

The FortiManager VM subscription license supports FortiManager version 6.4.1 and later. For information about supported firmware, see FortiManager VM firmware on page 11.

You can use the FortiManager VM subscription license with new FMG-VM installations.

For existing FMG-VM installations, you cannot upgrade to a FortiManager VM subscription license. Instead, you must migrate data from the existing FMG-VM to a new FMG-VM with subscription license.

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 6.4.3.

Supported models for MEA

You can use any of the following FortiManager models as a host for management extension applications:

FortiManager	FMG-3000F, FMG-3000G, FMG-3700F, FMG-3900E, and FMG-4000E.
FortiManager VM	FMG-VM64, FMG-VM64-Ali, FMG-VM64-AWS, FMG-VM64-AWSOnDemand, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

Minimum system requirements

Some management extension applications supported by FortiManager 6.4.3 have minimum system requirements. See the following table:

Management Extension Application	Minimum system requirement
SD-WAN Orchestrator	At least 12GB of memory is recommended to support SD-WAN Orchestrator MEA.
Wireless Manager (WLM)	A minimum of 4 CPU cores and 8 GB RAM is typically required. Depending on the number of running applications, the allocated resources should be increased.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 6.4.3.

Policy Hit Count on unused policy

FortiManager 6.4.3 and later no longer displays policy hit count information on the *Policy & Objects* > *Policy Packages* pane. However, you can view hit count information by using the *Unused Policies* feature and clearing the *Unused Only* checkbox. For more information, see the FortiManager 6.4 New Features Guide.

Wireless Manager (FortiWLM) not accessible

If Wireless Manager was enabled in FortiManager 6.4.0, you can no longer access it in the FortiManager GUI when you upgrade FortiManager to 6.4.2. When you try to access FortiWLM, you are redirected to the FortiManager dashboard.

SD-WAN Orchestrator not accessible

If SD-WAN Orchestrator was enabled in FortiManager 6.4.1, you can no longer access it in the FortiManager GUI after upgrading to FortiManager 6.4.2.

To workaround this issue, run the following CLI command to manually trigger an update of SD-WAN Orchestrator to 6.4.1 r2:

```
diagnose docker upgrade sdwancontroller
```

Support for FortiOS 6.4 SD-WAN Zones

In 6.4 ADOMs, SD-WAN member interfaces are grouped into SD-WAN zones. These zones can be imported as normalized interfaces and used in firewall policies.

FortiGuard Rating Services with FortiGate 6.4.1 or Later

FortiManager 6.4.1 or later is the supported version to provide FortiGuard rating services to FortiGate 6.4.1 or later.

Citrix XenServer default limits and upgrade

Citrix XenServer limits ramdisk to 128M by default. However the FMG-VM64-XEN image is larger than 128M. Before updating to FortiManager 6.4, increase the size of the ramdisk setting on Citrix XenServer.

To increase the size of the ramdisk setting:

1. On Citrix XenServer, run the following command:
   ```
   xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912
   ```
2. Confirm the setting is in effect by running `xenstore-ls`.
   ```
   ----------------------
   limits = ""
   pv-kernel-max-size = "33554432"
   pv-ramdisk-max-size = "536,870,912"
   boot-time = ""
   ---------------------------
   ```
3. Remove the pending files left in `/run/xen/pygrub`.

The ramdisk setting returns to the default value after rebooting.

Multi-step firmware upgrades

Prior to using the FortiManager to push a multi-step firmware upgrade, confirm the upgrade path matches the path outlined on our support site. To confirm the path, please run:

```
dia fwmanager show-dev-upgrade-path <device name> <target firmware>
```

Alternatively, you can push one firmware step at a time.

Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
set ssl-protocol t1sv1
```

```
    end
```

Upgrade Information

You can upgrade FortiManager 6.2.0 or later directly to 6.4.3.

For other upgrade paths and details about upgrading your FortiManager device, see the *FortiManager Upgrade Guide*.

This section contains the following topics:

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. In addition the local password is erased.

A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}
execute format {disk | disk-ext4 | disk-ext3}
```

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Aliyun

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FMG_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.

Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FMG_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

Microsoft Hyper-V 2016 is supported.

VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

For more information see the FortiManager product data sheet available on the Fortinet web site, http://www.fortinet.com/products/fortimanager/virtualappliances.html. VM installation guides are available in the Fortinet Document Library.

SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager version 5.00 file folder.

Product Integration and Support

This section lists FortiManager 6.4.3 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

FortiManager 6.4.3 support

This section identifies FortiManager 6.4.3 product integration and support information:

To confirm that a device model or firmware version is supported by the current firmware version running on FortiManager, run the following CLI command:

```
diagnose dvm supported-platforms list
```

Always review the Release Notes of the supported platform firmware version before upgrading your device.

Web browsers

This section lists FortiManager 6.4.3 product integration and support for web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 81
- Google Chrome version 86

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS/FortiOS Carrier

This section lists FortiManager 6.4.3 product integration and support for FortiOS/FortiOS Carrier:

- 6.4.0 to 6.4.3
- 6.2.0 to 6.2.5
- 6.0.0 to 6.0.10

FortiADC

This section lists FortiManager 6.4.3 product integration and support for FortiADC:

- 6.0.1
- 5.4.3

FortiAnalyzer

This section lists FortiManager 6.4.3 product integration and support for FortiAnalyzer:

- 6.4.0 and later
- 6.2.0 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

FortiAuthenticator

This section lists FortiManager 6.4.3 product integration and support for FortiAuthenticator:

- 6.0 to 6.2
- 5.0 to 5.5
- 4.3 and later

FortiCache

This section lists FortiManager 6.4.3 product integration and support for FortiCache:

- 4.2.9
- 4.1.6
- 4.0.4

FortiClient

This section lists FortiManager 6.4.3 product integration and support for FortiClient:

- 6.4.0 and later
- 6.2.8
- 5.6.6
- 5.4.0 and later

FortiDDoS

This section lists FortiManager 6.4.3 product integration and support for FortiDDoS:

- 5.3.1
- 5.2.0
- 5.1.0
- 5.0.0
- 4.7.0
- 4.6.0
- 4.5.0
- 4.4.2
- 4.3.2
- 4.2.3

Limited support. For more information, see Feature support on page 18.

FortiMail

This section lists FortiManager 6.4.3 product integration and support for FortiMail:

- 6.0.10
- 5.4.11
- 5.3.13

FortiSandbox

This section lists FortiManager 6.4.3 product integration and support for FortiSandbox:

- 3.1.4
- 3.0.6
- 2.5.2
- 2.4.1

- 2.3.3
- 2.2.2

FortiSOAR

This section lists FortiManager 6.4.3 product integration and support for FortiSOAR:

- 6.4.0 and later
- 6.0.0 and later

FortiSwitch ATCA

This section lists FortiManager 6.4.3 product integration and support for FortiSwitch ATCA:

- 5.2.3
- 5.0.0 and later

FortiWeb

This section lists FortiManager 6.4.3 product integration and support for FortiWeb:

- 6.3.7
- 6.2.3
- 6.1.2
- 6.0.7
- 5.9.1
- 5.8.6
- 5.7.2
- 5.6.1
- 5.5.6
- 5.4.1

Virtualization

This section lists FortiManager 6.4.3 product integration and support for virtualization:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2012 and 2016
- Nutanix AHV (AOS 5.10.5)
- OpenSource XenServer 4.2.5
- VMware ESXi versions 5.0, 5.5, 6.0, 6.5 , 6.7, and 7.0

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiADC		✓		
FortiAnalyzer			✓	✓
FortiAuthenticator				✓
FortiCache			✓	✓
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓
FortiSandbox		✓	✓	✓
FortiSOAR		✓		
FortiSwitch ATCA	✓			
FortiWeb		✓	✓	✓
Syslog				✓

Language support

The following table lists FortiManager language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Spanish		✓

To change the FortiManager language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *Administrative Settings* > *Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages by exporting a predefined language from FortiManager, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiManager. For more information, see the *FortiAnalyzer Administration Guide*.

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 6.4.3.

Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

This section contains the following topics:

FortiGate models

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-2200E, FortiGate-2201E, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate DC:**FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC **FortiGate Hardware Low Encryption:** FortiGate-100D-LENC **FortiWiFi:** FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-60F, FortiWiFi-61F, **FortiGate VM:** FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV,FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen **FortiGateRugged:** FortiGateRugged-60F, FortiGateRugged-60F-3G4G	6.4
FortiGate: FortiGate-30E, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FG-60E-DSL, FortiGate-60E-POE, FortiGate-61E, FortiGate-60F, FortiGate-61F, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-101E, FortiGate-100F, FortiGate-101F, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FG-400E, FG-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1100E, FortiGate-1101E, FortiGate-2000E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3700D, FortiGate-3800D,FortiGate-2200E, FortiGate-2201E, FortiGate-2200E, FortiGate-2201E, FortiGate-3300E, FortiGate-3301E, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1	6.2

Model	Firmware Version
FortiGate DC: FortiGate-80C-DC, FortiGate-401E-DC, FortiGate-600C-DC, RortiGate-800C-DC, FortiGate-800D-DC, FortiGate-1000C-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3240C-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600C-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC **FortiGate Hardware Low Encryption:** FortiGate-80C-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC **FortiWiFi:** FortiWiFi-30D, FortiWiFi-30D-POE, FortiWiFi-30E, FortiWiFi-30E-3G4G-INTL, FortiWiFi-30E-3G4G-NAM, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-80CM, FortiWiFi-81CM, FortiWiFi-60F, FortiWiFi-61F **FortiGate-VM:** FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AWSONDEMAND, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager **FortiGate Rugged:** FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D, FortiGateRugged-60F, FortiGateRugged-60F-3G4G **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-GBL, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FortiGate-60F, FortiGate-61F, FG-60F, FG-61F, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FortiGate-100F, FortiGate-101F, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FortiGate-2200E, FortiGate-2201E, FG-2500E, FortiGate-3300E, FortiGate-3301E, FG-3000D, FG-3100D, FG-3200D, FG-3600C, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E **FortiGate 5000 Series:** FG-5001D, FG-5001E, FG-5001E1 **FortiGate DC:** FG-401E-DC, FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3600E-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC **FortiGate Hardware Low Encryption:** FG-100D-LENC, FG-600C-LENC **Note:** All license-based LENC is supported based on the FortiGate support list. **FortiWiFi:** FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D, FortiWiFi-60F, FortiWiFi-61F, **FortiGate VM:** FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-Azure, FG-VM64-GCP,VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM, FOS-VM64-Xen **FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D	6.0

FortiGate special branch models

Model	Firmware Version
FortiWiFi: FortiWiFi-40F, FortiWiFi-40F-3G4G	6.4
FortiGate: FortiGate-30E-3G4G-GBL, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81F, FortiGate-1800F, FortiGate-1801F, FortiGate-4200F, FortiGate-4201F **FortiGate 6000 Series:** FortiGate-6000F **FortiGate 7000 Series:** FortiGate-7000E **FortiGate Rugged:** FortiGateRugged-90D **FortiWiFi:** FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWifi-60E-DSL, FortiWiFi-60E-DSLJ,	6.2
FortiGate: FortiGate-30E-3G4G-GBL, FortiGate-41F, FortiGate-41F-3G4G, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60F, FortiGate-61F, FortiGate-400E, FortiGate-401E, FortiGate-600E, FortiGate-601E, FortiGate-1800F, FortiGate-1801F, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E **FortiGate 6000 Series:** FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F **FortiGate 7000 Series:** FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC **FortiGate DC:** FortiGate-1100E-DC, FortiGate-3400E-DC, FortiGate-3401E-DC **FortiGate VM:** FortiGate-VM64-RAXONDEMAND **FortiWiFi:** FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-41F, FortiWiFi-41F-3G4G,	6.0

FortiCarrier models

Model	Firmware Version
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3400E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier-DC:** FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC **FortiCarrier-VM:** FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.4
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1	6.2

Model	Firmware Version
FortiCarrier-DC: FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC **FortiCarrier-VM:** FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3700D, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001D, FGT-5001E **FortiCarrier-DC:** FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC **FortiCarrier-VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	6.0

FortiADC models

Model	Firmware Version
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	6.0
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	5.4

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E **FortiAnalyzer VM:** FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWSOnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand,FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	6.4

Model	Firmware Version
FortiAnalyzer: FAZ-200F, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-1000E, FAZ-2000E, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3700F and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-Ali, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-GCP, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-OPC, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	6.2
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	6.0
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	5.6
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B. **FortiAnalyzer VM:** FAZ-VM64, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	5.4
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	5.0

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000B, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	4.3, 5.0-5.5, 6.0
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	4.0-4.2

FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3000E, FCH-3900E **FortiCache VM:** FCH-VM64, FCH-KVM	4.0, 4.1, 4.2

FortiDDoS models

Model	Firmware Version
FortiDDoS: FortiDDoS-200B, FortiDDoS-400B, FortiDDoS-600B, FortiDDoS-800B, FortiDDoS-900B, FortiDDoS-1000B, FortiDDoS-1200B, FortiDDoS-1500E, FortiDDoS-2000B, FortiDDoS-2000E	5.2, 5.3
FortiDDoS: FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-1500B, FI-2000B, FI-2000E	5.1
FortiDDoS: FI-1500E, FI-2000E	5.0
FortiDDoS: FI-200B, FI400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B	4.0, 4.1, 4.2, 4.3, 4.4, 4.5, 4.7

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-400E, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM, FML-200F, FML-400F, FML-900F	6.0
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E **FortiMail Low Encryption:** FE-3000C-LENC	5.4
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B **FortiMail Low Encryption:** FE-3000C-LENC **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.1

Model	Firmware Version
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.0

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E **FortiProxy VM:** FPX-KVM, FPX-VM64	1.0, 1.1, 1.2

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox-VM:** FSA-AWS, FSA-VM	3.1
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-AWS, FSA-VM	3.0
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-KVM, FSA-VM	2.5.2
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-VM	2.4.1 2.3.3
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D **FortiSandbox VM:** FSA-VM	2.2.0 2.1.3
FortiSandbox: FSA-1000D, FSA-3000D **FortiSandbox VM:** FSA-VM	2.0.3 1.4.2
FortiSandbox: FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

FortiSOAR models

Model	Firmware Version
FortiSOAR VM: FSR-VM	6.4
FortiSOAR VM: FSR-VM	6.0

FortiSwitch ATCA models

Model	Firmware Version
FortiController: FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-5913C	5.2.0
FortiSwitch-ATCA: FS-5003A, FS-5003B **FortiController:** FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3.0 4.2.0

FortiWeb models

Model	Firmware Version
FortiWeb: FortiWeb-100D, FortiWeb-400C, ortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.2, 6.3
FortiWeb: FortiWeb-100D, FortiWeb-400C, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XenServer	6.1
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-600D, FWB-1000D, FWB-1000E, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM, FWB-HYPERV, FWB-XENOPEN, FWB-XENSERVER	6.0.1
FortiWeb: FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.9.1
FortiWeb: FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.8.6

Model	Firmware Version
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7.2
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.6.1
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.6
FortiWeb: FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV	5.4.1
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, and FWB-HYPERV	5.3.9
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-HYPERV,FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER	5.2.4

Resolved Issues

The following issues have been fixed in 6.4.3. For inquires about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
587879	AP Manager central mode is missing AP group with VLAN ID.
607107	FortiManager prompts installation errors when certain channels are selected for *Radio 2* in *5 GHZ band* of *FAP-421E*.
607170	*Dynamic VLAN* option is not saved in SSID in AP Manager.
608870	Changing FortiAP setting to override *radio 1 TX power* control from *auto* to *manual* generates incorrect configuration causing install to fail.
610724	Unauthorized APs should be displayed so that users can authorize the APs.
645030	Adding FortiGate using custom admin profile may fail to list FortiAP in AP Manager.
645713	FortiManager is able to create SSID which cannot be deleted.
653329	FortiManager sends the wrong device setting after changing the FortiAP name.
654171	There may be duplicate entries in *objcfg_wireless_controller_wtp* not allowing the user to delete some custom WTP profiles.
663983	FortiAP upgrade may not proceed past 20%.
665945	Brazil country (BR) code does not offer any radio choices.

Device Manager

Bug ID	Description
552492	VAP is always loading under CLI configuration.
595058	When customer sets *Scheduled Updates* configuration to *1 hour* in FortiGuard on Device Manager, FortiManager installation preview is configured as *set time 1:60*.
605688	The character limit for `pac-file-data`is set to `4000` under CLI Configuration.
613029	SD-WAN Monitor is showing effect of exceeded SLA even when it is disabled.

Bug ID	Description
614953	Device dashboard reboot and shutdown operations may not work.
627749	Admin users with *device-config* set as *read* in the admin profile cannot download configuration revision.
635316	Return button is not working when viewing HA mode.
635701	Blocked address, trusted address, disabled signature and disabled-sub-class lists are not displayed on WAF profile CLI Configuration.
635738	FortiManager should show a clear message when it fails to load device configuration.
639854	No IPv6 format in router GUI for BGP.
644596	FortiManager is unable to deauthorize explicit proxy user(s).
646609	Devices may disappear randomly after upgrade.
649157	Mapping interface containing "/" results error *Object does not exist* during import policy.
649566	CLI Template is not able to install same name interface using `vpn ipsec phase1-interface` and `config system ipsec-aggregate`.
649769	FortiManager cannot view full list of Extenders.
650545	Import may get stuck in an infinite loop when there is a recursive reference.
650987	Interface template may show an empty action list.
651186	DNS widget may be empty under system template.
651712	SD-WAN monitor keeps loading and not displaying anything in backup mode ADOM.
652481	Allow access is missing under interface on AWS FortiGate and may cause installation to fail.
653331	Device Manager may not be able to open the NTP page.
653388	IPsec VPN Phase-1 tunnel interface is not added in VDOM interface list with a long VDOM name.
653465	FortiManager may not be able to edit DHCP options function on GUI.
653701	When FortiManager is configured in advanced ADOM mode, FortiManager still allows device assignment of CLI Templates/Groups in an ADOM where the management VDOM of that device does not reside in that particular ADOM.
656200	SD-WAN rule may not show all internet services.
656650	Import policy may fail due to local certificate.
657335	When creating VLAN interface with non-management VDOM, no interfaces can be listed.
657988	FortiManager may lose connection and fail to install after FortiGate HA switching roll.
659838	Interfaces *any* and *virtual-wan-link* should not be visible as OSPF passive interface option.
659862	FortiManager sends *unset serial* for FortiAnalyzer settings when *System Template* is being used.

Bug ID	Description
660662	FortiManager should support increased user local and user group member on FortiGate model 400E or 900E.
661116	Device configuration may not be updated after running CLI script on remote FortiGate.
662073	FortiManager should create a new OSPF interface when clicking the *OK* button.
662095	FortiManager may take a long time to send SLA updates to more than a thousand FortiGate devices.
664999	Importing a policy from FortiGate may not complete.
665013	After upgrade, FortiManager may not be able to refresh multiple devices at once.
667142	FortiManager is unable to edit or mouse over OSPF route after the seventh line.
668315	Maximum device group section can create more than specified by device group license limit.
668664	Policy package diff is much slower after upgrade.
668958	After enabling DHCP relay on one interface, DHCP server is disabled on another interface during install.
670072	FortiManager can export license file but it does not include HA information.
671139	FMG-VM64-AWSOnDemand may show serial number as *FMG-VM0000000000* with valid license status.

FortiSwitch Manager

Bug ID	Description
651788	FortiSwitch Manager does not show the correct online or offline status.
659568	FortiSwitch may not be visible under FortiSwitch Manager.

Global ADOM

Bug ID	Description
645702	Global policy install should not show warnings when a policy package has no installation target.
657642	FortiManager is unable to replace firewall object in Global Header Policy using the option *Find and Replace*.
666842	Cloning a global policy package may fail with *runtime error -1: invalid value*.

Others

Bug ID	Description
596067	In `workflow` mode, FortiManager cannot add devices to policy package installation target via JSON API.
632822	The `merged_daemons` process goes to 100% usage and prevents radius authentication.
647156	FortiManager cannot clone any of the `deep-inspection` ssl-ssh-profiles using JSON API.
647488	When using the Wireless Manager, FortiManager automatically returns to the main page after about 20 seconds.
657450	Docker interface range may create network conflict with the user's network.
657566	After upgrade, copy may fail for central SD-WAN with configuration error, *error service - 2 :-2 - Please assign a member*.
662965	Error may occur when checking and repairing invalid object sequence with `diagnose cdb upgrade check`.
663476	FortiManager is unable to configure system admin *ssh-public-key* via JSON API.
664554	HA sync error may print repeatedly on secondary FortiManager.
665424	Add an option in FortiManager CLI to skip unmapped normalized interface for input-device.

Policy and Objects

Bug ID	Description
525625	When configuring web filter rating override, the configuration is pushed to all the VDOMs even when the web filter is not used.
531112	Consolidated policy is missing implicit deny policy.
583151	FortiManager should not change default value of scan-mode and ssl-ssh-profile/inspection-mode when installing v6.0 policy package to v6.2.
599129	While editing policy from Policy Package, it is not possible to select SSL/SSH Inspection profile.
600165	Firewall consolidated policy is still named *SSL Inspection & Authentication* when it is profile based.
607958	FortiManager should be able to modify per-device mapping for global VIP in local ADOM.
609389	Within the anti-virus profile, the *Send Files to FortiSandbox Appliance for Inspection* option should not always be set to *None*.
618321	FortiManager is unable to create RSSO Group if the agent is configured with custom name.

Bug ID	Description
620092	*Interface Pair View* is not working for *Security Policies*.
623833	Username cannot exceed 35 characters.
631372	Setting `server-cert-mode` to replace may cause install failure if `inspect-all` is `certificate-inspection`.
632771	Users may not be updated on FortiManager after a new session is created on ISE.
634241	VIP created using CLI script is not available to use in a policy.
635966	Azure SDN connector only fetches the first page of results.
639437	FortiManager intermittently not displaying custom objects inside of address group.
640157	Verification may fail due to wrong default setting of `log.memory.global-setting'> set max-size`.
644689	FortiManager may not be able to load application control profile.
645058	Existing objects may disappear while editing policy and adding new one in batch mode.
646583	*Policy Lookup* should be available on GUI.
651785	Address section under *Policy & Objects* > *Security Profiles* > *SSL/SSH Inspection*" may load indefinitely.
651820	FortiManager should remove interface reference check for normalized interface per-device mapping.
654609	FortiManager is unable to create and display destination of imported internet service custom object.
655248	*Policy Consistency Check* may return duplicate address object names.
656206	FortiManager may not be able to add a proxy policy and it may not be able to search on source address field.
656324	Policy object panel search may not work on source user group field.
657826	FortiManager should not allow unsupported options in *Certificate Inspection* SSL/SSH inspection profiles to be visible.
657896	FortiManager should provide more descriptive error message when copy fails.
661268	Renaming address object may bypass the length check.
663219	FortiManager may not be able to add more than 10240 service objects.
664307	Cloning DNS filter profile that is assigned from Global ADOM results in Response with errors.

Revision History

Bug ID	Description
586275	*Policy Package Diff* does not show user or admin details.
587682	Installing mobile token that does not belong to target FortiGate may fail.
611536	IPsec Phase1 dhgrp and proposal settings may be ignored for FortiOS v5.2 devices after FortiManager is upgraded.
612263	FortiManager may not install ADSL vci and VPI to FWF-60E-DSL.
614485	FortiManager should support the configuration, `set initiator-ts-narrow enable`.
622540	FortiManager prompts error, *'no hub configured*, for a site even when the site is not part of VPN Manager.
634345	Install preview may not show CLI configurations correctly.
647180	Install copy may fail with error message *ftgd-wf - - The category is already set in another filter*.
649662	Installation may fail due to *cert-validation-timeout* setting error when installing v6.2 policy package to v6.4 FortiGate.
650017	Install fails for adding md5-key on OSPF interface when default authentication is set as *None*.
650239	Installation fails with *wireless-controller vap mesh-backhaul* setting despite setting being disabled on FortiManager.
652337	VPN Manager changes may result in unnecessary FortiGate configuration changes.
654496	Installing configuration to device after Auto link, FortiManager may send incorrect system ntp commands causing install to fail.
656505	Install may fail for *youtube-channel-filter* after creating a web filer profile.
656645	Copy may fail due to missing Health Check in device database.
656713	FortiManager may try to delete dynamically generated EMS firewall addresses which causes install failure.
657344	Installing from 6.0 ADOM may try to *unset inspection-mode* and *unset ssl-ssh-profile* on FortiGate 6.2.
657424	FortiManager may disable the *l2forward* and *stpforward* settings on virtual switch interface when installing policy package.
657526	FortiManager should not try to unset *ssl-ssh-profile* configuration if it is already configured.
662438	FortiManager may try to purge all web rating override entries.

Script

Bug ID	Description
592660	Running a script remotely may trigger a full configuration retrieve instead of a partial configuration retrieve.
611396	After it is locked on a device, FortiManager cannot show the list of devices to run a script.
629722	FortiManager cannot set system admin password with ENC format via CLI template.
632014	When editing CLI script group, user cannot see the full CLI script name.
669198	Running a script in Policy & Objects does not update *Save* status.

Services

Bug ID	Description
437935	FAD-VM license may not be validated on FortiManager.
587730	FortiGate-VM64-AZURE may not be listed in firmware image page.
603414	FortiManager may show incorrect firmware upgrade path.
652764	In FortiManager, *Enforce Firmware Version* may fail to upgrade FortiGate to a custom build.
654129	FortiManager may not have the correct upgrade path for FortiGate KVM.
666716	FortiGuard license status page should have an option to show all FortiGate HA cluster contracts.

System Settings

Bug ID	Description
489837	Certificate request CRS does not include the SAN DNS.
556334	Standard ADOM users should be able to assign system templates to FortiGate devices.
579727	Removing *enrollment method* from local certificate.
589203	ADOM upgrade from 5.6 to 6.0 may fail due to invalid per-device mapping.
596212	SSH filter profile is unset in firewall profile group upon ADOM upgrade.
597917	*Mail Server* setting within *Event Handler Notifications* is not synchronized from FortiManager to managed FortiAnalyzer.

Bug ID	Description
611215	SNMP Hosts in SNMP Community are not displayed in the GUI if ADOM is unlocked.
619750	When upgrading ADOM from 5.4 to 5.6, FortiManager does not add *tcp-session-without-syn* in all firewall policies.
624354	There may be an empty space in ADOM management page.
639099	There are many *cdb event log for object changed* in event logs after upgrade.
640505	Remote admin authentication with RADIUS may stop working.
650326	After HA failover, the new primary device may have incorrect policies.
654370	Users may not be able to access Java console with an error message: *Too many concurrent connections*.
654637	After upgrade, non *super_user* password changes may not taking effect.
655515	FortiManager may not be able to clone the Security Fabric ADOM.
656703	FortiManager requesting AuthnContext *PasswordProtectedTransport* causes errors if IdP is Azure AD with MFA.
657403	ADOM upgrade to 6.4 may hang and cause *cdb* reader to crash.
657664	FortiManager may not be able to upgrade ADOM from 6.2 to 6.4 when *Policy Block* is used.
657843	FortiManager needs to handle IPv6 policy migration with policy block.
658689	Log service may shutdown and restarted routinely.
660226	HA may crash when upgrading.
660361	ADOM upgrade may fail when FortiManager has `workspace-mode` set to `workflow`.
665033	Global web rating overrides may not be assigned after upgrade.
665356	Event logs should not contain users are not responsible for synchronizing device manager database between FortiManager and FortiAnalyzer.
667961	The *View SP Metadata* button for single sign-on may not response.

VPN Manager

Bug ID	Description
647413	Customer should be able to select the OS to allow or deny an SSL-VPN tunnel connection.
650454	Installation may fail when *Dialup VPN* interface is *PPPoE* logical interface.
648067	VPN Manager needs to support dynamic address group that has nested dynamic address objects.

Known Issues

The following issues have been identified in 6.4.3. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
667215	FortiManager should be able to classify Rogue FortiAPs.
669906	FortiManager may not be able to install mpsk-key from AP Manager.

Device Manager

Bug ID	Description
575215	When creating a new interface for a VDOM, FortiManager may list interfaces that may belong to another ADOM.
598431	Install wizard may show a blank area when scrolling down the wizard to select device(s).
609744	*Device Manager* > *System* > *Interface* may not be able to delete SSID interface.
627664	FortiManager cannot cooperate with *socket-size 0* and changes it to *1* automatically.
636012	Importing a policy may report conflict for the default SSH CA certificates.
636357	Retrieve may fail on FortiGate cluster with *Failed to reload configuration. invalid value* error.
645086	Policy Lookup shows an error even though the device is in sync.
646421	FortiManager may not be able to configure VDOM property resources setting.
649785	*SD-WAN* > *Monitor* may hang for an ADOM with 1500 devices.
649821	Installation may fail for FortiGate-600D.
652052	FortiManager may fail to add another FortiManager in Fabric ADOM.
654190	FortiManager should not modify IPv4 addressing mode when IPv6 addressing mode is changed.
655264	VDOM count is not correct when `vdom-mode split-vdom` is configured on FortiGate with VM0xV license.
659387	FortiManager should be able to provision CLI-template, SD-WAN-template, and Policy

Bug ID	Description
	Package together to the model device.
659981	FortiManager should be able to identify and show default SSL-SSH profile as read-only profiles.
662243	FortiManager is unable to clone SNMP Community under *System Templates*.
664253	The *auto-join-forticloud* configuration may cause *out-of-sync* status.
665955	FortiManager is not reflecting proper *admintimeout* value in CLI only object.
666833	GUI returns no warning when 4-byte AS or invalid community being configured on Standard community.
666872	BGP Neighbors table does not have height limit and vertical scroll bar.
667738	GUI should generate error message when using invalid IP address or special characters in interface name.
669129	FortiManager does not create dynamic mapping for address group causing import failure.
669155	SD-WAN monitor hangs while loading when admin profile is set to *Read-Only* for SD-WAN.
669704	FortiManager does not allow the user to configure FortiGate admin password longer than 32 characters.
670535	Install fails when creating a new DHCP reservation, due to missing MAC address.
670577	When creating an API admin from CLI Configuration, *Trusted Host* section is missing.
670839	FortiManager should be able to configure IPSec Phase2 selector using the same IP range.
671348	FortiManager should allow more than ten incoming source interfaces for policy routing decision.
672338	FortiManager may unset interface weight in SD-WAN when installing within 6.0 ADOM.
674904	FortiManager may not be able to import policy with interface binding contradiction on *srcintf* error.

FortiSwitch Manager

Bug ID	Description
650453	FortiSwitch template and VLAN shall appear for firewall policy creation.

Global ADOM

Bug ID	Description
632400	When installing a global policy, FortiManager may delete policy routes and settings on an ADOM.
667197	User should not be able to delete global object when ADOM is not locked.
667423	Assigned header policy from the global ADOM shows up on excluded policy package.
670280	Promoting the *Profile Group* object should not promote the default *Protocol* option.

Others

Bug ID	Description
659916	FortiManager may consume high memory usage by the *svc sys* daemon.
661069	ADOM restricted access user is able to pull Device Manager information from ADOMs via JSON API.
665617	FortiManager may consume high CPU resource when locking ADOM or loading policy.

Policy & Objects

Bug ID	Description
565301	Exporting policy package to Excel may not work.
612317	FortiManager shows incorrect country code for Cyprus under *User definition*.
623100	FortiManager is constantly changing UUID for firewall address object.
652753	When an obsolete internet service is selected, FortiManager may show entry IDs instead of names.
658528	The URL remote category, *FortiGuard Threat Feed*, is not available in the drop down menu for *Proxy Address*.
669389	Install may fail due to web filter profile in flow mode with setting changes available in proxy mode only.
670019	There is no *Decrypted Traffic Mirror* option in policy when only one port mapping is enabled in Full SSL/SSH Inspection.
670061	FortiManager does not report error when an unsupported FQDN address format is created.

Bug ID	Description
670833	Search box for address may not always work.
671265	Global object assignment may not work.
671988	FortiManager is not able to push dynamic objects to FortiGate after received the configurations from NSXT connector.
673305	Policy package install may stuck and fail due to high memory usage.
675541	Deleting an override entry should trigger modified status for policy packages with *FortiGuard Category Based Filter* enabled within web filter profile.

Revision History

Bug ID	Description
601229	FortiManager is missing *device-type* option for *custom device* dynamic mapping.
615936	FortiManager is missing the SSH protocol in DLP filter.
637103	Scrolling in *Install Preview* is not smooth and may get stuck.
647189	FortiManager dynamic object filter generator is adding a "s" at the end of tag resulting in non working object.
651991	After adding and removing Security Profile, policy Security Profile change from no-inspection to empty.
657026	GUI stuck in loading when trying to apply changes made to Anti Virus profile.
660483	IPS signatures may not match between FortiGate and FortiManager.
661590	Without selecting security profile group on proxy policy, FortiManager should fail to install with a proper error message.
664284	FortiManager may not be able to configure SSH certificate.
666258	User should not be able to create a firewall policy with an Internet service with Destination direction in *Source* by using drag and drop.
666913	Web URL Filter is deleted when *URL Filter* option is unchecked under the *Web Filter Profile*.
667148	When a policy install is performed, Install preview shows lot of firewall policies with metafield changes without any actual change been done.
667414	FortiManager may freeze when editing the comment field on a policy package with many policies.
673327	With traffic shaper in Mbps or Gbps, FortiManager should convert it to Kbps if installation target is non 64 bits FortiGate model.
675867	The ssl-anomaly-log configuration may incorrectly pushed by FortiManager when installing 5.6 ADOM policy to 6.0 FortiGate.

Script

Bug ID	Description
668947	Changes using CLI Script may not be applied to devices in the container or folder.
637465	Installation fails when installing global v6.2 IPv4 policy to v6.4 FortiGate.
660525	Installing from FortiManager, it may undo *comment*, *organization*, and *subnet-name* during the install.
662661	Default value of *global: system npu ip-reassembly:max-timeout* NPU setting in ADOM 6.0 for FortiGate-1800F should be changed to *10000* to avoid Conflict status.
663820	The LDAP port value remains *636* on device database and FortiManager is not accepting custom port number via CLI script.

Services

Bug ID	Description
591748	Hide or show license expired devices may not work.
671387	FortiManager installs the latest IPS and application control signatures on managed device despite the *To Be Deployed Version* is configured.

System Settings

Bug ID	Description
489837	Certificate request CRS does not include the SAN DNS.
489837	Certificate request CRS does not include the SAN DNS.
623457	FortiManager prompts error while importing CA certificate.
631733	Changing *trusted IP* can be saved and installed.
642205	While FortiAnalyzer model is disabled, FortiManager may fail to create an ADOM due to over size with disk quota.
652417	FortiManager HA may go out of synchronization periodically based on the logs.
660130	ADOM upgrade may fail caused by invalid setting of *ssl-exempt*.
662970	Firewall addresses may not be not visible on GUI after upgraded FortiManager.
667445	FortiManager may show errors on *dynamic_mapping.local-int* during upgrade.
677118	Upgrading ADOM from 6.2 to 6.4 may fail due to replacement message.

VPN Manager

Bug ID	Description
596953	When the user goes to *VPN manager > Monitor*, and selects a specific community from the tree menu to show only that community's tunnels, the monitor page displays a white screen.
608221	There is no *XAUTH USER* column in *VPN Manager Monitor*.
653328	FortiManager is unable to edit a SSL portal in VPN Manager containing "/" special character.
658221	The *dns-suffix* on SSL VPN portal is not installed if web-mode is disabled.

Appendix A - FortiGuard Distribution Servers (FDS)

In order for the FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as a FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the items listed below:

- FortiManager accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between FortiManager and FDS, FortiManager uses port 80 to communicate with the proxy server by default and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through via port 443.

FortiGuard Center update support

You can configure FortiManager as a local FDS to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform/version:

Platform	Antivirus	WebFilter	Vulnerability Scan	Software
FortiClient (Windows)	✓	✓	✓	✓
FortiClient (Mac OS X)	✓		✓	
FortiMail	✓			
FortiSandbox	✓			
FortiWeb	✓			

To enable FortiGuard Center updates for FortiMail version 4.2 enter the following CLI command:

```
config fmupdate support-pre-fgt-43
set status enable
end
```